



## Daily Open Source Infrastructure Report 03 August 2015

### Top Stories

- The General Motors Company confirmed July 30 that OnStar-equipped vehicles are vulnerable to a flaw that could allow an attacker to remotely locate the vehicle and issue commands through OnStar's RemoteLink app. – *CNET* (See item [3](#))
- Matson Navigation Company agreed to reimburse the State of Hawaii more than \$15 million in cleanup costs and restoration fees following a 2013 incident in which a faulty loading pipeline leaked 1,400 tons of molasses into the Honolulu Harbor. – *Reuters* (See item [5](#))
- The July 29 Rocky fire in Lake County, California reached 15,000 acres by July 30, burning parts of the Cache Creek Wilderness Area and the Snow Mountain National Monument Area, and forcing the evacuation of 650 people. – *Sacramento Bee* (See item [9](#))
- Two California residents were indicted July 30 on charges alleging they were conspirators to a 2011 cyberattack in which 94,000 credit and debit card numbers were stolen from Michaels Stores Inc., customers. – *Reuters* (See item [16](#))

---

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

#### SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

#### SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL and STATE

- [Government Facilities](#)
  - [Emergency Services](#)
-

## **Energy Sector**

1. *July 30, Los Angeles Times* – (California) **Power restored in Long Beach except for about 400 customers.** An underground electrical vault explosion in Long Beach, California forced crews to shut down 3 additional substations in order to make repairs July 30, cutting power to 30,000 customers. No injuries were reported, although one home was damaged in the explosion.  
Source: <http://www.latimes.com/local/lanow/la-me-ln-long-beach-outages-20150730-story.html>
2. *July 30, Associated Press* – (Nevada) **Vegas-area coal plant owners to pay \$4.3M to settle lawsuit.** Operators of the Reid Gardner Power Generation Station outside Las Vegas agreed July 28 to pay a \$4.3 million settlement over allegations from neighboring Moapa Band of Paiute Indians of health problems and water pollution caused by contaminants from the station.  
Source: <http://www.ktnv.com/story/29672247/vegas-area-coal-plant-owners-to-pay-43m-to-settle-lawsuit>

## **Chemical Industry Sector**

Nothing to report

## **Nuclear Reactors, Materials, and Waste Sector**

Nothing to report

## **Critical Manufacturing Sector**

3. *July 30, CNET* – (National) **GM quickly issues fix for OnStar hack, but service still vulnerable.** The General Motors Company confirmed July 30 that OnStar-equipped vehicles are vulnerable to a flaw that could allow an attacker to remotely locate the vehicle and issue commands through OnStar's RemoteLink app, such as locking doors or starting the engine. A hacker demonstrated the vulnerability using a device called "OwnStar," which he claimed allowed him to intercept communications between the app and the vehicle.  
Source: <http://www.cnet.com/news/ownstar-onstar-hack/>

## **Defense Industrial Base Sector**

Nothing to report

## **Financial Services Sector**

4. *July 31, MarketWatch* – (National) **How vulnerable are the U.S. stock markets to hackers?** An analysis of information security and cyber risk trends in the financial sector cited findings from a 2015 U.S. Securities and Exchange Commission Risk Alert revealing that about 88 percent of brokerages and 74 percent of financial advisers in the

U.S. have suffered cyber-attacks, and that according to Congressional testimony, a major U.S. bank is attacked every 34 seconds, among other disclosures.

Source: <http://www.marketwatch.com/story/how-vulnerable-are-the-us-stock-markets-to-hackers-2015-07-31>

For another story, see item [16](#)

## **Transportation Systems Sector**

5. *July 30, Reuters* – (International) **Shipping company Matson to pay Hawaii \$15 million over molasses spill.** The Matson Navigation Company agreed to pay the State of Hawaii more than \$15 million in cleanup costs and restoration fees July 30 following a 2013 incident in which a faulty loading pipeline leaked 1,400 tons of molasses into the Honolulu Harbor, damaging the ecosystem and closing parts of the harbor for days.

Source: <http://www.reuters.com/article/2015/07/30/usa-molasses-hawaii-idUSL1N10A10920150730>

## **Food and Agriculture Sector**

For another story, see item [5](#)

## **Water and Wastewater Systems Sector**

For another story, see item [5](#)

## **Healthcare and Public Health Sector**

6. *July 31, WNBC 4 New York* – (New York) **Number of Legionnaires' cases rises amid deadly outbreak in NYC: officials.** Health officials announced July 30 an “unusual” spike in Legionnaire’s disease after 46 cases, including 2 fatalities, were reported in the south Bronx since July 10. Authorities do not believe the outbreak is connected to contaminated drinking water, and an investigation into cooling towers is being conducted across the area.

Source: <http://www.nbcnewyork.com/news/local/Legionnaires-Disease-Outbreak-New-York-City-Health-Officials-Pneumonia-320164021.html>

7. *July 30, St. Louis Post-Dispatch* – (Missouri) **BJC HealthCare hobbled by systemwide computer outage that lasted 20 hours.** A 20-hour computer outage at BJC HealthCare in St. Louis, Missouri July 28 – July 29 blocked access to electronic health records, email, registration and scheduling systems, and the system’s bed tracking system at the health system’s 13 hospitals, forcing employees to register patients and chart information with pen and paper. The exact cause of the outage has not yet been determined.

Source: [http://www.stltoday.com/business/local/bjc-healthcare-hobbled-by-systemwide-computer-outage-that-lasting-hours/article\\_dea221f0-fe39-59f9-93c9-60b6ac2633b9.html](http://www.stltoday.com/business/local/bjc-healthcare-hobbled-by-systemwide-computer-outage-that-lasting-hours/article_dea221f0-fe39-59f9-93c9-60b6ac2633b9.html)

## **Government Facilities Sector**

8. *July 30, Fresno Bee* – (California) **Wildfire spreads out of containment lines in Sequoia National Forest.** The Cabin wildfire in the Sequoia National Forest spread outside containment lines July 29, reaching over 800 acres by July 30 and prompting the closure of portions of the Golden Trout Wilderness.  
Source: <http://www.fresnobee.com/news/local/article29555605.html>
9. *July 30, Sacramento Bee* – (California) **Rocky fire grows to 15,000 acres burned, 5 percent contained.** The July 29 Rocky fire in Lake County, California reached 15,000 acres by July 30, burning parts of the Cache Creek Wilderness Area and the federal Snow Mountain National Monument Area and forcing the evacuation of 650 people. About 1,000 first responders, 150 fire engines, 8 airplanes, and 8 helicopters are scheduled to arrive onsite July 31.  
Source: <http://www.sacbee.com/news/state/california/fires/article29529397.html>

## **Emergency Services Sector**

10. *July 30, WHAS 11 Louisville* – (Indiana) **S. Ind. man accused of stealing of military items from National Guard Armory.** Indiana State police reported July 30 that a man broke into the New Albany National Guard Armory November 2014 and stole more than \$10,000 worth of equipment including tasers and pepper spray, among other military items, and tried to sell the equipment on various social media sites.  
Source: <http://www.whas11.com/story/news/crime/2015/07/30/military-items-stolen-sellersburg-indiana/30889585/>
11. *July 30, Tampa Tribune* – (Florida) **Fire breaks out in Bartow police evidence room.** A July 30 fire in the evidence room of the Bartow Police Department in Tampa prompted the building to be evacuated and the communication center to be moved to another building. Officials reported there will be no interruptions in police or fire services, but an investigation is ongoing to determine the cause of the fire.  
Source: <http://tbo.com/news/crime/fire-breaks-out-in-bartow-police-evidence-room-20150730/>
12. *July 30, Associated Press* – (Alabama) **Former police officer indicted on theft, extortion charges.** A former Prattville, Alabama police officer was indicted July 30 on charges of theft, possession of a controlled substance, extortion, and impersonating a police officer after stealing prescription medication from a pharmacy.  
Source: <http://www.wvtm13.com/news/former-police-officer-indicted-on-theft-extortion-charges/34445376>

For another story, see item [9](#)

## **Information Technology Sector**

13. *July 31, Help Net Security* – (International) **Cybercriminals are preying on existing vulnerabilities to plan future attacks.** An analysis of cyber threats by Solutionary

identified several campaigns consisting of over 600,000 events worldwide that targeted the bash vulnerability in the second quarter of 2015, and found that the U.S. was a leading source of command and control traffic and malware threats, among other findings.

Source: <http://www.net-security.org/secworld.php?id=18691>

14. *July 30, Securityweek* – (International) **Stack ranking the SSL vulnerabilities for the enterprise.** Security researchers discovered an OpenSSL vulnerability dubbed “OprahSSL” in which an attacker with a legitimate end-leaf certificate could circumvent OpenSSL code validating the certificate’s purpose, and sign other certificates in order to perpetrate man-in-the-middle (MitM) attacks on Secure Sockets Layer (SSL) sessions, and ranked the severity of the flaw in relation to other SSL vulnerabilities, including Heartbleed, Early CCS, and LOGJAM.

Source: <http://www.securityweek.com/stack-ranking-ssl-vulnerabilities-enterprise>

15. *July 30, Softpedia* – (International) **Google fixes Chrome issue that leaked the user’s real IP from behind a VPN.** Google released a Chrome Web browser extension called “WebRTC Network Limiter” to address an issue with the WebRTC protocol in which certain circumstances could reveal the real public and local Internet Protocol (IP) address of a user connected via a virtual private network (VPN).

Source: <http://news.softpedia.com/news/google-fixes-chrome-issue-that-leaked-the-user-s-real-ip-from-behind-a-vpn-488143.shtml>

For additional stories, see items [3](#) and [4](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

## Communications Sector

Nothing to report

## Commercial Facilities Sector

16. *July 31, Reuters* – (California) **Two charged in 2011 cyber breach at Michaels retailer.** Two California residents were indicted July 30 on charges alleging that they were conspirators to a 2011 cyberattack in which 94,000 credit and debit card numbers were stolen from Michaels Stores Inc., customers.

Source: <http://www.businessinsurance.com/article/20150731/NEWS06/150739970/two-charged-in-2011-cyber-breach-at-michaels-retailer?tags=>

17. *July 31, KYW 13 Philadelphia* – (National) **Seven indicted in NJ following large scale jewelry theft scheme.** Seven people were indicted July 31 on theft charges for

allegedly stealing more than \$800,000 in jewelry from trade show attendees across several States.

Source: <http://philadelphia.cbslocal.com/2015/07/31/seven-indicted-jewelry-theft/>

18. *July 30, KOMO 4 Seattle* – (Washington) **Residents run through flames to escape Seattle apartment fire.** A 2-alarm fire severely damaged a Central District apartment building in Seattle after smoking materials were improperly discarded July 29. No injuries were reported and damages total approximately \$250,000.

Source: <http://www.komonews.com/news/local/Residents-run-through-flames-to-escape-Seattle-apartment-fire-320225411.html>

19. *July 31, WVIT 30 New Britain* – (Connecticut) **Lightning strike sparks 3-alarm fire at Danbury Condos.** A 3-alarm fire damaged 9 condo units in Danbury, Connecticut after lightning struck the complex July 30. No injuries were reported and the fire was extinguished.

Source: <http://www.nbcconnecticut.com/news/local/3-Alarm-Fire-Reported-in-Danbury-320199591.html>

20. *July 30, Sacramento Bee* – (California) **Seven mobile homes reported destroyed in fire in marina near Isleton.** A July 30 fire destroyed 12 homes in a Sacramento mobile home park after beginning in a nearby forested area and later spreading into the park. No injuries were reported and fire crews contained the incident.

Source: <http://www.sacbee.com/news/local/crime/article29608168.html>

For another story, see item [9](#)

## **Dams Sector**

Nothing to report



**Department of Homeland Security (DHS)**  
**DHS Daily Open Source Infrastructure Report Contact Information**

**About the reports** - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

**Contact Information**

Content and Suggestions:

Send mail to [cikr.productfeedback@hq.dhs.gov](mailto:cikr.productfeedback@hq.dhs.gov) or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to [support@govdelivery.com](mailto:support@govdelivery.com).

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto:nicc@hq.dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

**Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.